IBM Security
Intelligence. Integration. Expertise.

IBM

【 研究会1】 2020に備えたサイバー対処

小講演:「インシデントにおける初動対応」

2019年12月9日(月)

日本アイ・ビー・エム株式会社
X-Force & Security Intelligence
Incident Response and Intelligence Service
徳田敏文

パネリスト・プロフィール

徳田 敏文（とくだ としふみ）

X-Force & Security Intelligence 部長
Incident Response and Intelligence Services (IRIS)
Japan Leader, IBM X-Force メンバー

略歴：

科学技術系ソフトウェアの設計・開発に10年以上従事した後、1999年にインターネットセキュリティシステムズ株式会社（ISS)に入社。システムの脆弱性研究および不正アクセス検知・防御システムの考案に従事するほか、脆弱性検査やペネトレーションテストを担当。 2001年、24時間365日の不正アクセスリモート監視事業であるマネージド・セキュリティー・サービス（MSS）を事業責任者として担当。セキュリティーオペレーションセンター（SOC）の構築・運用から人員教育まで幅広く担当した。2007年、日本IBMとの会社統合後、セキュリティーサービスの開発を手がける。現在、日本IBMのインシデント対応サービスである、X-Force Incident Response and Intelligence Services (IRIS)を担当し、自らもセキュリティーインシデント対応として、現地調査や各種分析調査を実施する。

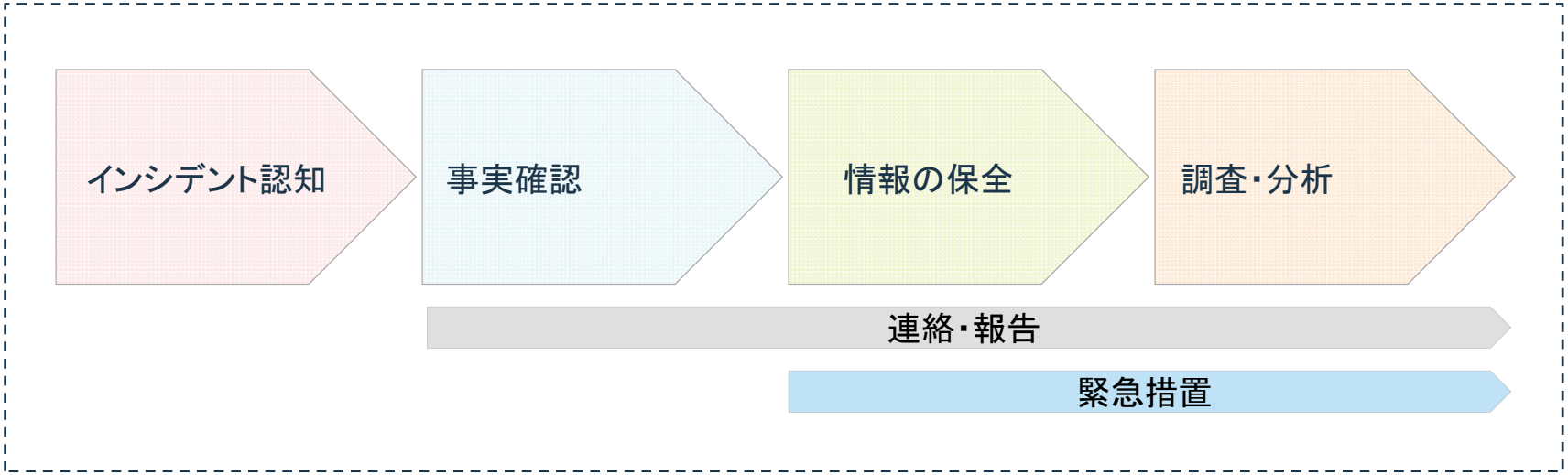
活動について：

- 情報処理安全確保支援士（第001894号）
- 情報処理技術者 ネットワークスペシャリスト、第1種情報処理
- 経済産業省商務情報政策局長表彰「情報セキュリティ部門」2010年
- 情報セキュリティ大学院大学客員研究員（2014～現任）
- サイバーセキュリティリスクと企業経営に関する研究会 委員 2015年
- 総合セキュリティ対策会議委員(警察庁 平成23,24,26年度）

- セキュリティー監視サービス企画立案・構築
- SOC構築支援
- 内部セキュリティ事故防止計画立案・支援
- サイバー犯罪者追跡等、情報漏えい事後対策
- インシデント対応
- セキュリティーインシデント対応サービス立案

小講演題:「インシデントにおける初動対応」

重要なサイバー対処のひとつに、セキュリティー・インシデントに直面した際に
どのような初動対応をするべきかが挙げられます。初動対応の遅れや誤りは、
インシデント全体の収束を遅らせるだけでなく対応コストの増大につながります。
最も重要な対応のひとつであるインシデントの初動対応で起こりやすい課題について
紹介します。



初動対応とは

インシデント認知後、本格的調査が実施される前の暫定対処等を含めた活動

- 事実確認を速やかに行う
- 何をまず行うべきなのか
- 今できる対応は、通信のブロック、ネットワーク分離、端末の回収
- 参照するマニュアルや規定はあるか、使えるか
- 自社のみで対応可能か
- 報告や連絡をどこまでするか
- 技術的な部分だけではない

事実確認

- 噂、想定、推測の排除
- 5W1H
- タイムラインの作成
- 機器・情報のリストアップ

情報の保全

- 揮発情報の保全
- 関係機材、機器の確保
- 当事者、関係者のリスト
- 先行ヒアリング

情報の統制

- 連絡や報告の範囲
- 共有範囲の設定

初動調査

- 検体やログの一次調査
- 通信のブロック
- 施設立ち入り調査
- 当事者ヒアリング

優先順位の決定

- 調査目的の設定
- 調査順や深さの決定
- 対応優先度決定

調査・分析

- 目的を持って調査
- 深掘りしすぎない
- 調査内容の共有
- 結果の共有

暫定対処の実施

- 応急処置の実施
- 機器の切り離し
- 通信のブロック

初動対応時に起こしやすいミス

- 揮発情報の喪失
- ログの消失
- AVや検疫システムによる検体等の消失
- 人為的ミスによるデータの消失
- 原因PCやデバイスなど関係機器の確保もれ
- 暫定措置の実施遅れによる2次被害の発生
- 調査・対応等優先順位の間違い
- バイアスによる調査方針の揺らぎ
- やりたくない理由を探す
- 責任者報告の遅れ（責任者不在）
- 当事者への情報漏れ

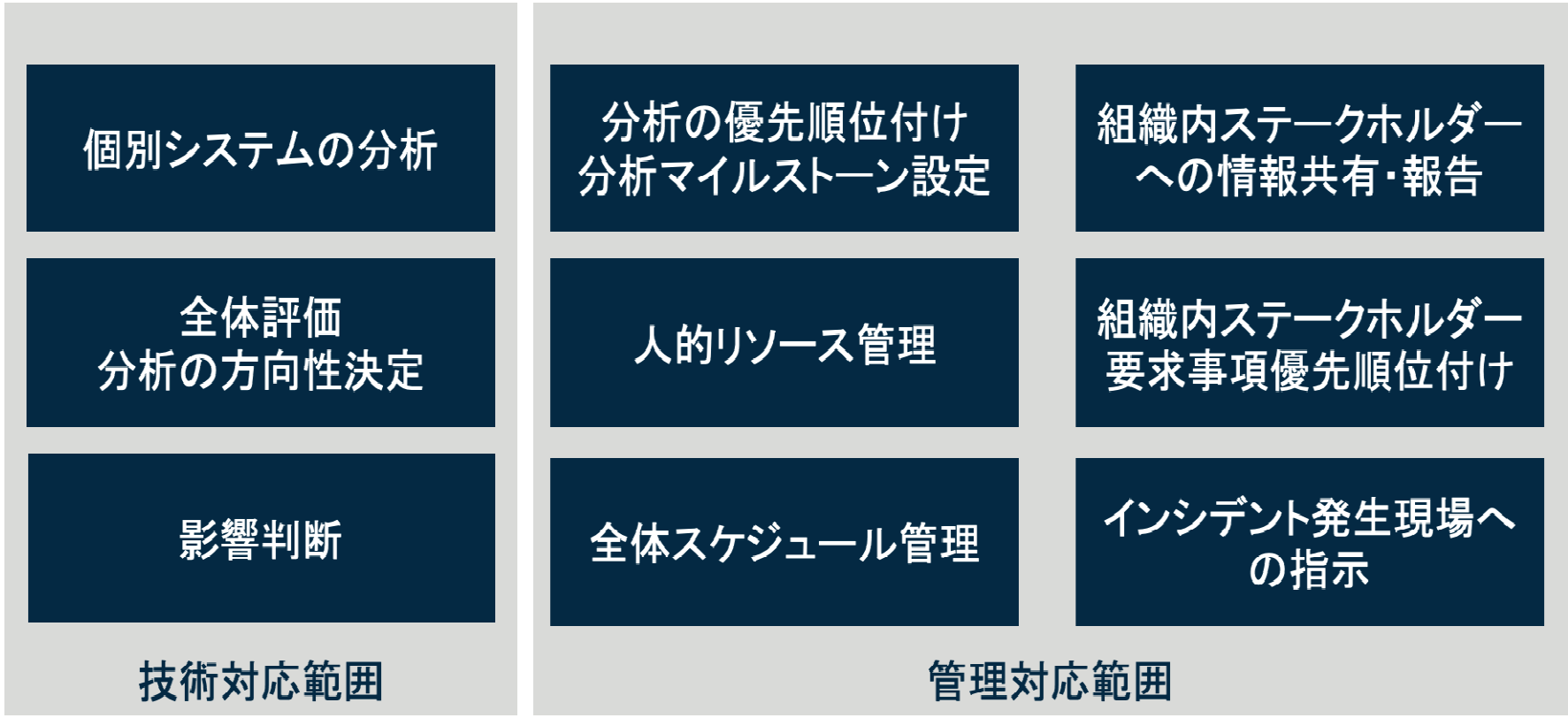
初動対応時に現場で生じる課題

- インシデント対応サービスとして現場に入った際に、次のような課題に遭遇する事がある。「インシデントが解決できない」「間違った結果を導き出してしまう」など、致命的な問題につながる場合がある

	インシデント現場の混乱	調査方針へのバイアス	内部漏えい対応不手際
課題	• 責任者不在 • インシデント対応経験がない • 事態を把握していない	• 都合による調査範囲の限定 • 欲しい結果への誘導 • 強引なシナリオの仮定	• データを全部渡さない • あるはずのログがない • 配慮のない当事者とのインタビュー
対策	✓ 状況を時系列でまとめて把握 ✓ 指揮命令系統の確認 ✓ 対応手順や関連規定等の確認 ✓ 連絡・報告	✓ 事実のみ取り扱う ✓ 必要以上の推測や仮定の排除 ✓ いつまでに何を実施するのか ✓ 結果に向き合う	✓ 時間を与えない ✓ データの保全を急ぐ ✓ 調査チームの動向を見せない ✓ 当事者との対面は避ける

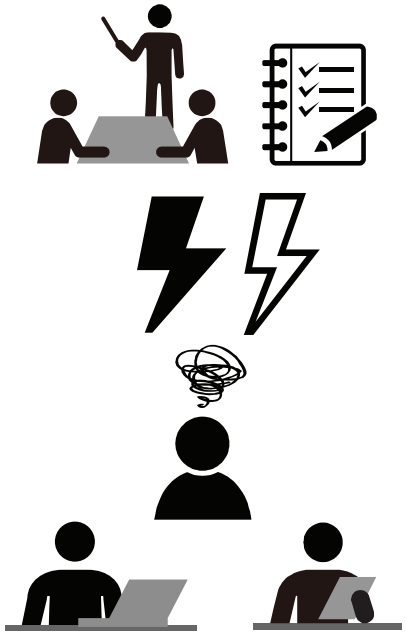
インシデント現場の混乱

- 最も大きな課題の一つは「責任者不在」である。責任者が明確化・周知されていなければ、現場で最も重要なものの一つである「優先順位の決定」が行われない
- 責任者の事態把握なしに、サービス事業者が調査や対応の優先順位を決めてしまうのは間違い



初動対応時の調査方針へのバイアス

- 上層部への説明を優先したい、あるいはインシデントのクローズをとにかく急ぎたいなどの理由で調査方針や方法・調査範囲にバイアスをかけられることも少なくない
- 強引なシナリオの設定は、「証拠の無視」が発生する



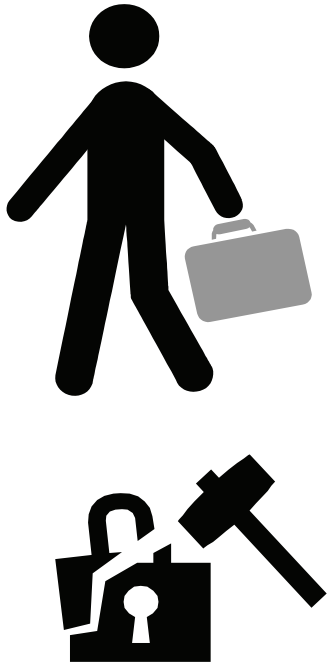
（例）

- A、B、C どれかのシナリオでマルウェアに感染したと上層部に報告したい
- シナリオを先に報告することによって、上層部からの説明要求に応えたい
- シナリオに合致しない「事実」は、別の理由と考えてしまう。
- 欲しい結果への誘導が発生する

科学的・論理的な調査により真実の追究を目指すべき

原因の当事者がいる場合の初動対応の不手際

- **故意による場合も事故による場合でも人的対応は細心の注意と計画を持って対応することが必要**



- 当事者とのインタビューの目的としては、事実関係の確認、情報の提供依頼（多くのケースでは私物PCの提供依頼）がある。その際、つい問い詰めたい気持ちが先走って叱責などをしてしまうと、証拠の隠滅、さらなる被害の拡大などにつながってしまう危険性がある。
- 故意の可能性がある場合は、物品の確保・回収は迅速に

当事者を大勢で取り囲む、叱責するなどの冷静さを失った対応はNG

重要なポイントは　～インシデント・マネジメント～

- **インシデントが起きてから対応するレスポンスの考えから、事前準備を含めて インシデントを管理するという考え方に移行する**

- インシデントは発生すると考え、対応を想定した準備を進めること
- インシデントが起きてから考えるのではなく普段から準備すること

事前に準備できること

- インシデント対応手順や初動対応フローなどを整備する
- ワークショップなどで実際に起こりうるインシデントを想定して訓練を実施してみる
- 信頼できるサービス・ベンダーを探しておく

対応するメンバーや関係者を集めて、インシデントが発生したと想定して 各自の考えや動きを確認しておくと良い。

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM